日本国特許庁
JAPAN PATENT OFFICE

10.07.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１０月　７日

出願番号
Application Number: 特願２００２－２９４１８４

[ST. 10/C]: [ＪＰ２００２－２９４１８４]

出願人
Applicant(s): 森井　昌克
小林　朗

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２００３年　８月１５日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３０６６４１３

【書類名】　特許願
【整理番号】　P02-157
【あて先】　特許庁長官殿
【国際特許分類】　G09C　1/00
　　G06F　7/58
【発明者】
　【住所又は居所】　徳島市助任本町３－２６
　【氏名】　森井　昌克
【発明者】
　【住所又は居所】　東大阪市新家中町１－８－９０６
　【氏名】　白石　善明
【特許出願人】
　【住所又は居所】　徳島市助任本町３－２６
　【氏名又は名称】　森井　昌克
【特許出願人】
　【住所又は居所】　兵庫県西宮市上ケ原四番町４番３３－７０８
　【氏名又は名称】　小林　朗
【代理人】
　【識別番号】　100100354
　【弁理士】
　【氏名又は名称】　江藤　聡明
【手数料の表示】
　【予納台帳番号】　119438
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　疑似乱数発生方法及び疑似乱数発生器

【特許請求の範囲】

【請求項１】　ｎ個のシフトレジスタを有し、１周期分のビット数が（２ｎ－１）個となるビット列を出力可能な線形フィードバックシフトレジスタの初期値を設定する第１ステップと、

所定の演算処理により前記初期値から前記線形フィードバックシフトレジスタの１周期分のビット数と互いに素である導出値を求める第２ステップと、

該導出値と前記線形フィードバックシフトレジスタの１周期分のビット数を２倍以上した値とを乗算して、前記第１線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出する第３ステップと、

前記算出したビット数分のビット列を前記線形フィードバックシフトレジスタから前記初期値をもとに出力させる第４ステップと、

該出力したビット列から前記導出値の間隔ごとにビット列を取り出して新ビット列を生成する第５ステップと、

該新ビット列を出力可能な構成に前記線形フィードバックシフトレジスタの構成を再構成する第６ステップと、

該再構成した後の線形フィードバックシフトレジスタから前記初期値をもとに疑似乱数を発生させる第７ステップと、

を有することを特徴とする疑似乱数発生方法。

【請求項２】　前記初期値に対してハッシュ関数を施してハッシュ値を求め、該ハッシュ値に最も近似した素数を導出値として採用することを特徴とする請求項１に記載の疑似乱数発生方法。

【請求項３】　前記線形フィードバックシフトレジスタの再構成は、バーレイキャンプマッセイアルゴリズムを用いて行われることを特徴とする請求項１または２に記載の疑似乱数発生方法。

【請求項４】　前記第７ステップで発生させた疑似乱数を非線形変換する第８ステップを有することを特徴とする請求項１～３のいずれかに記載の疑似乱数発生方法。

【請求項５】　ｎ個のシフトレジスタを有し、１周期分のビット数が（２ｎ－１）個となるビット列を出力可能な線形フィードバックシフトレジスタと、

秘密鍵に基づき前記線形フィードバックシフトレジスタの初期値を設定する初期値設定手段と、

所定の演算処理により前記初期値から前記線形フィードバックシフトレジスタの１周期分のビット数と互いに素である導出値を求める導出値算出手段と、

前記線形フィードバックシフトレジスタの１周期分のビット数を２倍以上した値と前記導出値とを乗算して、前記第１線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出するビット数算出手段と、

前記算出したビット数分のビット列を前記線形フィードバックシフトレジスタから前記初期値をもとに出力させるビット列出力手段と、

該出力したビット列から前記導出値の間隔ごとにビット列を取り出して新ビット列を生成する新ビット列生成手段と、

該新ビット列を出力可能な構成に前記線形フィードバックシフトレジスタの構成を再構成する線形フィードバックシフトレジスタ再構成手段と、

該再構成後の線形フィードバックシフトレジスタから前記初期値をもとに疑似乱数を発生させる疑似乱数発生手段と、を有することを特徴とする疑似乱数発生器。

【請求項６】　前記線形フィードバックシフトレジスタ再構成手段の代わりに、新ビット列を出力可能な構成を有する第２の線形フィードバックシフトレジスタを生成する線形フィードバックシフトレジスタ生成手段を設け、

前記疑似乱数発生手段は、前記第２の線形フィードバックシフトレジスタによって初期値をもとに疑似乱数を発生させることを特徴とする請求項５に記載の疑似乱数発生器。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、疑似乱数発生方法及び疑似乱数発生器に関し、特に暗号通信やデジタル署名などで利用する疑似乱数を発生させる疑似乱数発生方法及び疑似乱数発

生器に関する。

【０００２】

【従来技術】

従来より、有線や無線により情報通信を行う際に、内容が第三者に漏れないように情報を暗号化して送信することが行われている。この暗号化方式の一つに逐次暗号方式（ストリーム暗号方式）がある。逐次暗号方式は、送信側と受信側で同一の疑似乱数を発生させ、送信側は疑似乱数のビット列と平文のビット列とを用いて暗号文のビット列を作成し暗号文として受信側に送出し、受信側は送信側から受信した暗号文のビット列と疑似乱数のビット列とを用いて平文のビット列を求め平文に復号化するものである。

【０００３】

図４は、従来の逐次暗号方式を説明する図である。送信側の暗号化装置１００は、疑似乱数発生器１０１と論理演算処理部１０２を有しており、受信側の復号化装置１１０は、疑似乱数発生器１１１と論理演算処理部１１２を有している。

【０００４】

暗号化装置１００の疑似乱数発生器１０１と復号化装置１１０の疑似乱数発生器１１１は、同一の秘密鍵を与えることによって互いに全く同一の疑似乱数を発生する論理構造を有している。また、暗号化装置１００の論理演算処理部１０２と復号化装置１１０の論理演算処理部１１２は、ビット単位で排他的論理和の演算処理を行う。

【０００５】

図５は、暗号化装置１００の疑似乱数発生器１０１を説明する図である。尚、復号化装置１１０の疑似乱数発生器１１１については、暗号化装置１００の疑似乱数発生器１０１と同一の構成を有するのでその詳細な説明を省略する。

【０００６】

疑似乱数発生器１０１は、非線形コンバイナ型の疑似乱数発生器であり、図５に示すように、並列に配置した複数の線形フィードバックシフトレジスタ（ＬＦＳＲ）１０３と、非線形変換部１０４とを有しており、各線形フィードバックシフトレジスタ１０３から出力したビット列を非線形変換して疑似乱数を発生させ

る。本従来例では、各線形フィードバックシフトレジスタ１０３は、１回のシフト動作でそれぞれ１ビット（Ｘ１、Ｘ２、・・・X_L）を出力し、非線形変換部１０４は、各線形フィードバックシフトレジスタ１０３から入力されたビット列をもとに１ビットの疑似乱数を出力する構成を有している。

【０００７】

図６は、一般的な線形フィードバックシフトレジスタ１０３の構成を簡単に説明する図である。線形フィードバックシフトレジスタ１０３は、１ビットの情報を記憶できる複数のシフトレジスタ１０５と、複数の排他的論理和演算回路１０６とを有し、各シフトレジスタ１０５の出力と各排他的論理和演算回路１０６の一方の入力との間にはフィードバックタップ１０７が接続されている。フィードバックタップ１０７（c_{n-1}、c_{n-2}、・・・c_n）は、１のとき結線を示し、０のとき断線を示し、それぞれが予め１または０に定められている。

【０００８】

このシフトレジスタ１０５の個数をｎとすると、１つのシフトレジスタ１０５に注目したとき、出力系列の最大周期は、（2^n-1）となることが知られており、この系列をM系列という。例えば、図６に示す線形フィードバックシフトレジスタ１０３の場合、M系列を生成する特性多項式は、以下の式で表される。

【０００９】

$$C(x)=X^n+c_{n-1}X^{n-1}+\cdots+c_1X+1$$

上記の特性多項式で第１項目の指数ｎは線形フィードバックシフトレジスタの次数、すなわちシフトレジスタの個数を示し、２項目以降の指数部分は、フィードバックタップによる結線位置を示している。上記（１）式に示す特性多項式が原始多項式となるようにすれば、線形フィードバックシフトレジスタは、M系列を出力する。

【００１０】

尚、従来より、線形フィードバックシフトレジスタからの出力を排他的論理和等の演算処理によって変更することが提案されている（例えば、特許文献１参照。）。

【００１１】

【特許文献１】

特開平６－３４２２５７号

【００１２】

【発明が解決しようとする課題】

しかしながら、線形フィードバックシフトレジスタ１０３は、シフトレジスタ数の２倍の出力を観測することで、線形フィードバックシフトレジスタ１０３の構成、すなわちシフトレジスタ数及び結線位置と、初期値の全てを特定することが可能である。したがって、構成が固定された線形フィードバックシフトレジスタ１０３をそのまま疑似乱数発生器１０１に用いるには、暗号強度が弱く、安全性に問題がある。

【００１３】

また、線形フィードバックシフトレジスタ１０３は、特性多項式の変更によりシフトレジスタの結線位置や結線数を変更すると、線形フィードバックシフトレジスタの出力がM系列ではなく短周期となって暗号強度が低下するおそれがあることから、特性多項式は予めM系列を出力する値に固定されているのが常識であり、線形フィードバックシフトレジスタの構成を容易に変更することはできないと考えられている。

【００１４】

本発明は、上述の点に鑑みなされたものであり、その目的は、強い暗号強度を維持しつつ線形フィードバックシフトレジスタの構成を容易かつ動的に変更することができる疑似乱数発生方法及び疑似乱数発生器を提供することにある。

【００１５】

【課題を解決するための手段】

上記課題を解決する請求項１に記載の発明による疑似乱数発生方法は、ｎ個のシフトレジスタを有し、１周期分のビット数が（２ｎ－１）個となるビット列を出力可能な線形フィードバックシフトレジスタの初期値を設定する第１ステップと、所定の演算処理により初期値から線形フィードバックシフトレジスタの１周期分のビット数と互いに素である導出値を求める第２ステップと、導出値と線形フィードバックシフトレジスタの１周期分のビット数を２倍以上した値とを乗算

して、第１線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出する第３ステップと、その算出したビット数分のビット列を線形フィードバックシフトレジスタから初期値をもとに出力させる第４ステップと、その出力したビット列から導出値の間隔ごとにビット列を取り出して新ビット列を生成する第５ステップと、その新ビット列を出力可能な構成に線形フィードバックシフトレジスタの構成を再構成する第６ステップと、再構成した後の線形フィードバックシフトレジスタから初期値をもとに疑似乱数を発生させる第７ステップと、を有することを特徴とする。

【００１６】

請求項２の発明は、請求項１に記載の疑似乱数発生方法において、初期値に対してハッシュ関数を施してハッシュ値を求め、そのハッシュ値に最も近似した素数を導出値として採用することを特徴とする。

【００１７】

請求項３の発明は、請求項１または２に記載の疑似乱数発生方法において、線形フィードバックシフトレジスタの再構成は、バーレイキャンプマッセイアルゴリズムを用いて行われることを特徴とする。

【００１８】

請求項４の発明は、請求項１～３のいずれかに記載の疑似乱数発生方法において、第７ステップで発生させた疑似乱数を非線形変換する第８ステップを有することを特徴とする。

【００１９】

請求項５に記載の発明による疑似乱数発生器は、ｎ個のシフトレジスタを有し、１周期分のビット数が（２^{n}－１）個となるビット列を出力可能な線形フィードバックシフトレジスタと、秘密鍵に基づき線形フィードバックシフトレジスタの初期値を設定する初期値設定手段と、所定の演算処理により初期値から線形フィードバックシフトレジスタの１周期分のビット数と互いに素である導出値を求める導出値算出手段と、線形フィードバックシフトレジスタの１周期分のビット数を２倍以上した値と導出値とを乗算して、第１線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出するビット数算出手段と、その

算出したビット数分のビット列を線形フィードバックシフトレジスタから初期値をもとに出力させるビット列出力手段と、その出力したビット列から導出値の間隔ごとにビット列を取り出して新ビット列を生成する新ビット列生成手段と、その新ビット列を出力可能な構成に線形フィードバックシフトレジスタの構成を再構成する線形フィードバックシフトレジスタ再構成手段と、再構成後の線形フィードバックシフトレジスタから初期値をもとに疑似乱数を発生させる疑似乱数発生手段と、を有することを特徴とする。

【００２０】

請求項６に記載の発明は、請求項５に記載の疑似乱数発生器において、線形フィードバックシフトレジスタ再構成手段の代わりに、新ビット列を出力可能な構成を有する第２の線形フィードバックシフトレジスタを生成する線形フィードバックシフトレジスタ生成手段を設け、疑似乱数発生手段は、第２の線形フィードバックシフトレジスタによって初期値をもとに疑似乱数を発生させることを特徴とする。

【００２１】

【発明の実施の形態】

次に、本発明の実施の形態について図に基づいて説明する。

【００２２】

図１は、本実施の形態における疑似乱数発生器１を説明する図である。本実施の形態では、非線形コンバイナ型の疑似乱数発生器１を例に説明する。

【００２３】

疑似乱数発生器１は、利用者から与えられる秘密鍵に基づいて初期値を設定する初期値設定部（図示せず）と、初期値設定部から受け取った初期値をもとに疑似乱数を生成する複数の疑似乱数生成部１０と、これら複数の疑似乱数生成部１０の出力側に各々接続され、各疑似乱数生成部１０から出力される疑似乱数を非線形変換する非線形変換部２０を有している。

【００２４】

初期値設定部は、利用者から与えられる秘密鍵をビット列に変換し、疑似乱数生成部１０の数に分割して、後述する疑似乱数生成部１０の線形フィードバック

シフトレジスタ１１にそれぞれ割り当てる初期値を生成する処理を行う。

【００２５】

疑似乱数生成部１０は、Ｌ個が互いに並列に配置されており、それぞれ線形フィードバックシフトレジスタ１１と、線形フィードバックシフトレジスタ再構成手段１２を有している。

【００２６】

線形フィードバックシフトレジスタ１１は、従来技術で説明したものと同様に、１ビットの情報を記憶できるｎ個のシフトレジスタと、排他的論理和演算回路を有している。そして、本実施の形態では、１周期分のビット数ｍが（２ｎ－１）個となるビット列、いわゆるM系列を出力可能な構成に予め設定されている。

【００２７】

図２は、本実施の形態における線形フィードバックシフトレジスタ１１の初期多項式を例示するものである。初期多項式は、M系列を出力するように予め設定されている特性多項式であり、１項目の指数部（図２では「＾」で表している）がシフトレジスタの個数を示し、２項目以降の指数部が排他的論理和演算回路に接続された結線位置を示している。例えば、１段目の線形フィードバックシフトレジスタ１１（ＬＦＳＲ１）は、１３１個のシフトレジスタを有し、８番目、３番目、２番目のシフトレジスタがフィードバックタップによって排他的論理和演算回路に接続されていることを示している。尚、本実施の形態では、シフトレジスタの個数ｎは、全て素数個に設定されている。

【００２８】

線形フィードバックシフトレジスタ再構成手段１２は、線形フィードバックシフトレジスタ１１の構成を秘密鍵によって動的に変更して再構成するものである。具体的には、出力系列がM系列のビット列をｓ個ごとにサンプルした新ビット列は、M系列の１周期分のビット数ｍ（＝２ｎ－１）と導出値ｓとが互いに素であるとき、すなわち、１以外の共通の約数を持たないときは、他の構成を有する線形フィードバックシフトレジスタのM系列になり、また、バーレイキャンプマッセイアルゴリズムによって、少なくとも２周期分以上のビット数を有するビット列から、そのビット列を出力可能な等価で最小の線形フィードバックシフトレ

ジスタの特性多項式を求めることができることを利用して、線形フィードバックシフトレジスタ１１の再構成を行う。

【００２９】

線形フィードバックシフトレジスタ再構成手段１２は、初期値設定部によって与えられた初期値から導出値ｓを算出し、導出値ｓと線形フィードバックシフトレジスタ１１の１周期分のビット数ｍ（＝２^{n}－１）を２倍した値２ｍとを乗算し、線形フィードバックシフトレジスタ１１から出力させるビット列のビット数２ｍｓを算出する。

【００３０】

そして、初期値をもとに線形フィードバックシフトレジスタ１１から２ｍｓ個のビット列を出力させ、その２ｍｓ個のビット列から導出値ｓの間隔ごとにビット列を取り出して新ビット列を生成し、その新ビット列を用いてバーレイキャンプマッセイアルゴリズムにより線形フィードバックシフトレジスタ１１の構成を変更する。

【００３１】

尚、本実施の形態では、線形フィードバックシフトレジスタ１１から出力させるビット列のビット数が２ｍｓ個である場合を例に説明しているが、新ビット列のビット数が２ｍ個以上であれば、等価な最小の線形フィードバックシフトレジスタを求めることができるので、２ｍｓ個以上であればよい。

【００３２】

バーレイキャンプマッセイアルゴリズムとは、線形フィードバックシフトレジスタ１１のシフトレジスタの個数ｎ（線形複雑度）の２倍以上のビット数を有するビット列を入手することで、そのビット列を出力可能な等価な最小の線形フィードバックシフトレジスタを得ることができるというアルゴリズムである。バーレイキャンプマッセイアルゴリズムについては、例えば、文献１「暗号理論入門（第２版）」、共立出版社、岡本栄司著、２００２年４月１０日発行、に詳細に説明されている。

【００３３】

次に、上記構成を有する疑似乱数発生器１の動作について図３のフローチャー

トを用いて以下に説明する。

【００３４】

まず最初に、初期値設定部によって初期値が設定される（ステップＳ１０１）。初期値は、利用者から与えられる秘密鍵を所定の演算処理によって分割することによって設定される。

【００３５】

例えば、秘密鍵の長さが１６バイトで「ＡＢＣＤＥＦＧＨＩＪＫＬＭＮＯＰ」であり、疑似乱数生成部１０が８段の場合には、初期値は下記のように設定される。

【００３６】

ＬＦＳＲ１　ＡＢ＋Ｘ’ＦＦ’埋め込み文字（Ｐａｄｄｉｎｇ）
ＬＦＳＲ２　ＣＤ＋Ｘ’ＦＦ’埋め込み文字（Ｐａｄｄｉｎｇ）
ＬＦＳＲ３　ＥＦ＋Ｘ’ＦＦ’埋め込み文字（Ｐａｄｄｉｎｇ）
ＬＦＳＲ４　ＧＨ＋Ｘ’ＦＦ’埋め込み文字（Ｐａｄｄｉｎｇ）
ＬＦＳＲ５　ＩＪ＋Ｘ’ＦＦ’埋め込み文字（Ｐａｄｄｉｎｇ）
ＬＦＳＲ６　ＫＬ＋Ｘ’ＦＦ’埋め込み文字（Ｐａｄｄｉｎｇ）
ＬＦＳＲ７　ＭＮ＋Ｘ’ＦＦ’埋め込み文字（Ｐａｄｄｉｎｇ）
ＬＦＳＲ８　ＯＰ＋Ｘ’ＦＦ’埋め込み文字（Ｐａｄｄｉｎｇ）

ここでは、初期値は、秘密鍵「ＡＢＣＤＥＦＧＨＩＪＫＬＭＮＯＰ」を、「ＡＢ」、「ＣＤ」、・・・、「ＯＰ」の２文字ずつに分割し、残りのシフトレジスタを埋め込み文字（Ｐａｄｄｉｎｇ）で埋めることによって設定される。

【００３７】

初期値設定部において秘密鍵から初期値が設定されると、各初期値は、各疑似乱数生成部１０にそれぞれ入力され、線形フィードバックシフトレジスタ１１のシフトレジスタ内にセットされる。

【００３８】

次に、線形フィードバックシフトレジスタ再構成手段１２によって、線形フィードバックシフトレジスタ１１の構成を再構成する処理が行われる（ステップＳ１０２～ステップＳ１０６）。

【００３９】

ここでは、まず、所定の演算処理により初期値から線形フィードバックシフトレジスタ１１の１周期分のビット数ｍと互いに素である導出値ｓを算出する（ステップＳ１０２）。導出値ｓは、初期値に対して、例えばＭＤ５などのハッシュ関数を施してハッシュ値を求め、そのハッシュ値に最も近似した素数が採用される。導出値ｓは、初期値から求めることができ、かつビット数ｍと互いに素であればよく、上記の算出方法によって求められるものに限定されない。但し、秘匿性を維持するために、上記所定の演算処理は、一方向性を満足しうる演算処理でなければならない。

【００４０】

導出値ｓを算出すると、次に、線形フィードバックシフトレジスタ１１から出力させるビット列のビット数２ｍｓを算出する（ステップＳ１０３）。線形フィードバックシフトレジスタ１１から出力させるビット列のビット数２ｍｓは、線形フィードバックシフトレジスタ１１の１周期分のビット数ｍ（＝２ｎ－１）を２倍した値と、導出値ｓとを乗算することによって求められる。

【００４１】

そして次に、線形フィードバックシフトレジスタ１１から初期値をもとに２ｍｓ個のビット数を有するビット列を出力させ（ステップＳ１０４）、そのビット列から新ビット列を生成する（ステップＳ１０５）。新ビット列は、２ｍｓ個のビット列から導出値ｓの間隔ごとに取り出したビット列によって構成され、そのビット数は２ｍ個となる。

【００４２】

ここで、出力系列がM系列のビット列をｓ個ごとにサンプルしたビット列は、そのM系列の１周期分のビット数ｍと導出値ｓとが互いに素であれば、他の構成を有する線形フィードバックシフトレジスタのM系列となることから、この新ビット列も、M系列となる。

【００４３】

そして、その新ビット列に基づいて線形フィードバックシフトレジスタ１１の構成を再構成する（ステップＳ１０６）。線形フィードバックシフトレジスタ１

１の再構成は、バーレイキャンプマッセイアルゴリズムを用いて行われる。バーレイキャンプマッセイアルゴリズムによれば、少なくとも２周期分以上のビット数を有するビット列があれば、かかるビット列を出力可能な等価で最小の線形フィードバックシフトレジスタを求めることができるので、２ｍ個のビット数を有する新ビット列から新たな線形フィードバックシフトレジスタの特性多項式を導出して、再構成を行う。

【００４４】

再構成後の線形フィードバックシフトレジスタ１１は、再構成前と同一の次数及び異なる結線の特性多項式を有し、同一の初期値を与えた場合に、再構成前と異なるM系列を出力可能な構成を有する。

【００４５】

線形フィードバックシフトレジスタ再構成手段１２による線形フィードバックシフトレジスタ１１の再構成が終了すると、再構成された線形フィードバックシフトレジスタ１１から初期値をもとに疑似乱数を発生させる処理が行われる（ステップＳ１０７）。これにより、疑似乱数生成部１０から再構成前とは異なるM系列の疑似乱数が発生される。

【００４６】

各疑似乱数生成部１０から出力された疑似乱数は、それぞれ非線形変換部３０に入力され、非線形変換部３０で所定の非線形関数ｆ（ｘ）に基づいて非線形変換される（ステップＳ１０８）。これにより、疑似乱数に非線形性を与えることができ、暗号強度を更に向上させることができる。

【００４７】

上記構成を有する疑似乱数発生器１によれば、線形フィードバックシフトレジスタ１１の構成を初期値に基づいて容易かつ動的に変更することができ、変更後もM系列を出力させることができる。したがって、解読者は、再構成前の線形フィードバックシフトレジスタの構成を取得することができない。これにより、従来、線形フィードバックシフトレジスタの構成が既知であることを前提に成り立っていた既存の暗号解読法は、成立しなくなる。したがって、高い暗号強度を得ることができ、情報の秘匿性を保つことができる。

【００４８】

尚、本発明は、上述の実施の形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲で種々の変更が可能である。例えば、上述の実施の形態では、非線形コンバイナ型の疑似乱数発生器１を例に説明したが、非線形コンバイナ型でなく、線形フィードバックシフトレジスタを用いる疑似乱数発生器であればよく、例えばブロック型暗号方式に用いられる疑似乱数発生器に用いてもよい。

【００４９】

また、上記のステップＳ１０６で、新ビット列に基づいて線形フィードバックシフトレジスタ１１の構成を再構成する代わりに、新ビット列を出力可能な構成を有する第２の線形フィードバックシフトレジスタを生成し、ステップＳ１０７で、その第２の線形フィードバックシフトレジスタによって初期値をもとに疑似乱数を発生させてもよい。これによれば、線形フィードバックシフトレジスタを２つに分けることができ、より秘匿性の向上を図ることができる。

【００５０】

また、本実施の形態における疑似乱数発生器１は、ソフトウエアやハードウエアのいずれによって構成してもよい。

【００５１】

【発明の効果】

以上説明したように、本発明に係る疑似乱数発生方法によれば、出力系列がM系列のビット列をｓ個ごとにサンプルしたビット列は、そのM系列の１周期分のビット数ｍ（＝２^{n}－１）と導出値ｓが互いに素であるときには、他の構成を有する線形フィードバックシフトレジスタのM系列を構成し、また、少なくとも２周期分以上のビット数を有するビット列から線形フィードバックシフトレジスタを求めることができることを利用して、線形フィードバックシフトレジスタの構成を初期値に基づいて動的に変更することができ、変更後の線形フィードバックシフトレジスタからM系列のビット列を出力させることができる。

【００５２】

したがって、解読者は、疑似乱数発生器から出力される疑似乱数に基づいて再構成前の線形フィードバックシフトレジスタの構成を得ることができず、初期値

や秘密鍵も解読することができない。この結果、高い暗号強度を得ることができ、情報の秘匿性を保つことができる。

【図面の簡単な説明】

【図１】

本実施の形態における疑似乱数発生器を説明する図である。

【図２】

本実施の形態における線形フィードバックシフトレジスタの初期多項式を例示するものである。

【図３】

本実施の形態における疑似乱数発生器の動作を説明するフローチャートである。

【図４】

従来の逐次暗号方式を説明する図である。

【図５】

従来の非線形コンバイナ型の疑似乱数発生器を概略的に示す図である。

【図６】

一般的な線形フィードバックシフトレジスタの構成及び動作を簡単に説明する図である。

【符号の説明】

１　疑似乱数発生器

１０　疑似乱数生成部

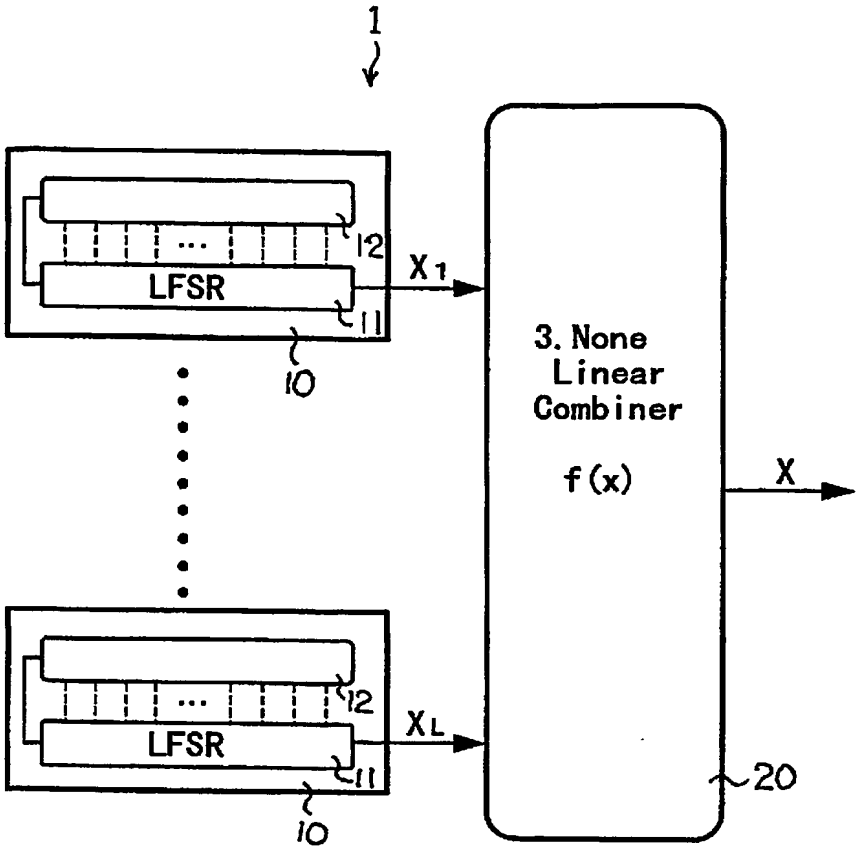
１１　線形フィードバックシフトレジスタ

１２　線形フィードバックシフトレジスタ再構成手段

２０　非線形変換部

【書類名】　　図面

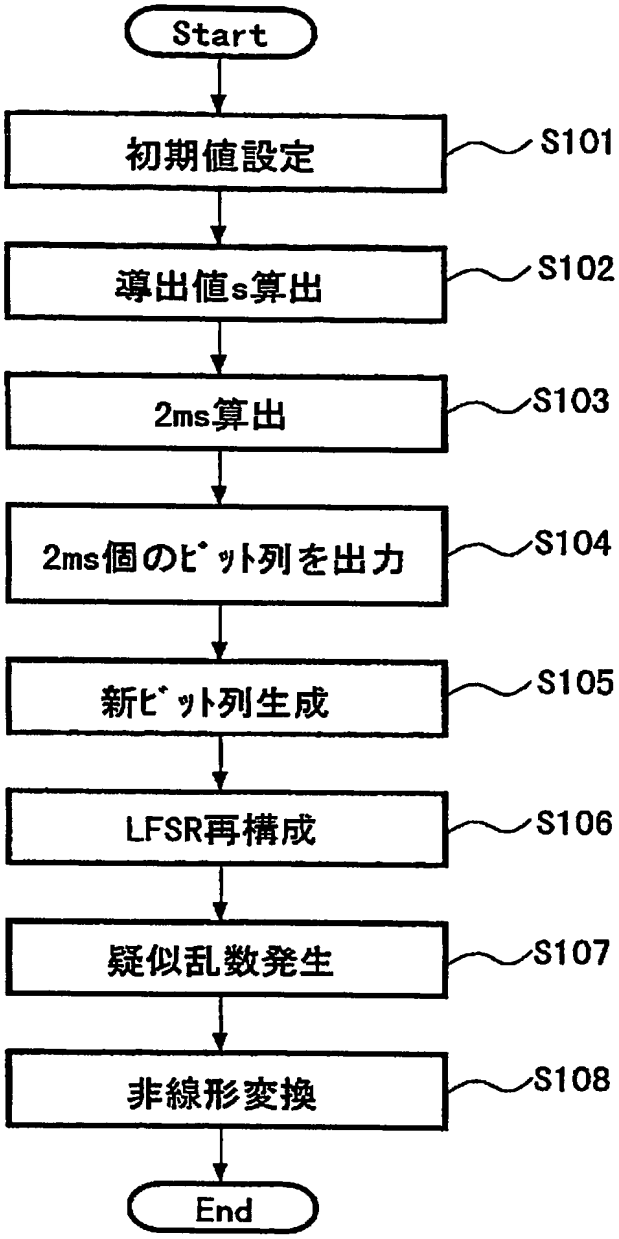
【図１】



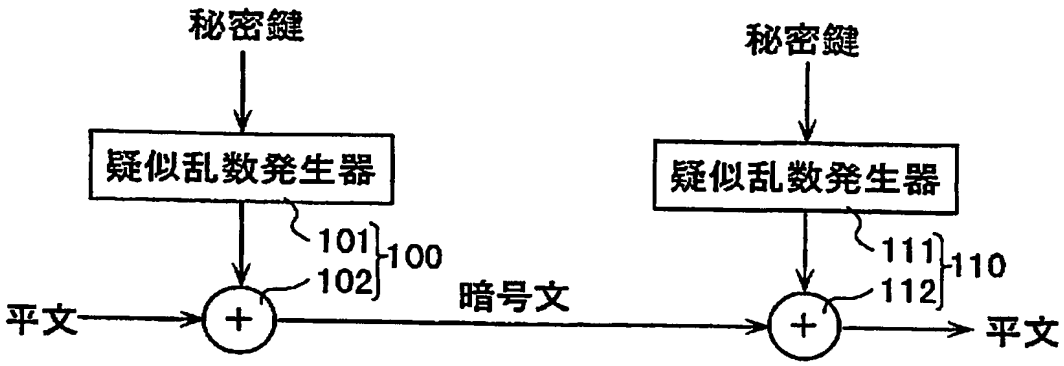
【図２】

LSFR1	x^131+x^8+x^3+x^2+1
LSFR2	x^137+x^21+1
LSFR3	x^139+x^8+x^5+x^3+1
LSFR4	x^149+x^10+x^9+x^7+1
LSFR5	x^151+x^3+1
LSFR6	x^157+x^6+x^5+x^2+1
LSFR7	x^163+x^7+x^6+x^3+1
LSFR8	x^167+x^6+1

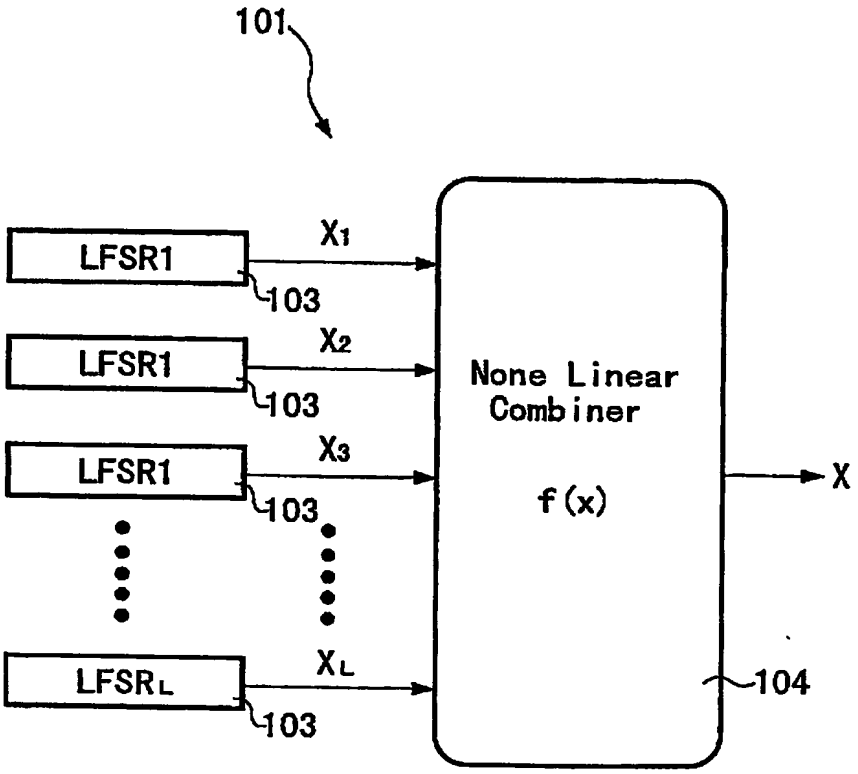
【図３】


Start
初期値設定
S101
導出値s算出
S102
2ms算出
S103
2ms個のﾋﾞｯﾄ列を出力
S104
新ﾋﾞｯﾄ列生成
S105
LFSR再構成
S106
疑似乱数発生
S107
非線形変換
S108
End

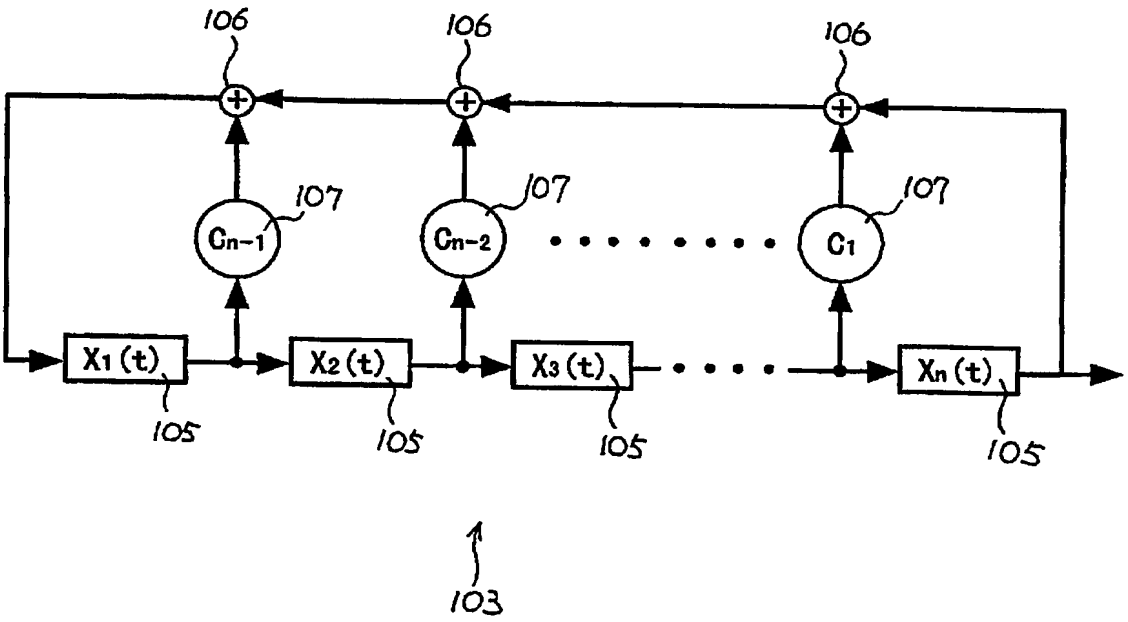
【図４】


秘密鍵
疑似乱数発生器
101
102
100
平文
暗号文
秘密鍵
疑似乱数発生器
111
112
110
平文

【図５】


101
LFSR1
X1
103
LFSR1
X2
103
LFSR1
X3
103
LFSRL
XL
103
None Linear
Combiner
f(x)
X
104

【図６】


106
106
106
107
107
107
Cn-1
Cn-2
C1
X1(t)
X2(t)
X3(t)
Xn(t)
105
105
105
105
103

【書類名】　要約書

【要約】

【課題】線形フィードバックシフトレジスタの構成を容易かつ動的に変更することができる疑似乱数発生方法を提供する。

を得ること。

【解決手段】出力系列がM系列のビット列をｓ個ごとにサンプルしたビット列は、そのM系列の１周期分のビット数ｍと導出値ｓが互いに素であるときは、他の構成を有する線形フィードバックシフトレジスタのM系列になり、また、少なくとも２周期分以上のビット数を有するビット列から最小で等価の線形フィードバックシフトレジスタを求めることができることを利用して、初期値に基づき線形フィードバックシフトレジスタ１１の構成を容易かつ動的に変更する。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００２－２９４１８４
受付番号	５０２０１５０９７９１
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１４年１０月１０日

＜認定情報・付加情報＞

【提出日】　平成14年10月 7日

次頁無

特願２００２－２９４１８４

出　願　人　履　歴　情　報

識別番号　　［５００００３０５３０］

１．変更年月日　　２０００年　１月２０日
［変更理由］　　新規登録
住　所　　徳島県徳島市助任本町３２６
氏　名　　森井　昌克

２．変更年月日　　２００３年　５月２８日
［変更理由］　　住所変更
住　所　　徳島県徳島市助任本町３－２６
氏　名　　森井　昌克

特願２００２－２９４１８４

出　願　人　履　歴　情　報

識別番号　　［５０２３６４８００］

１．変更年月日　　２００２年１０月　７日
［変更理由］　　新規登録
住　所　　兵庫県西宮市上ケ原四番町４番３３－７０８
氏　名　　小林　朗